PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Quibus International AB, Malmö SE*

(21) *Patentansökningsnummer* / *Patent application number* — *0400131-9*

(86) *Ingivningsdatum* / *Date of filing* — *2004-01-21*

Stockholm, 2005-01-24

För Patent- och registreringsverket
For the Patent- and Registration Office

Görel Gustafsson

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

METOD OCH ANORDNING FÖR ATT EFFEKTIVISERA SKYDDANDET AV ELEKTRONISKA DATA MOT PIRATKOPIERING I NÄTVERK SAMT UNDGÅ FILTRERINGSSYSTEM

UPPFINNINGSOMRÅDET

Metod för att effektivisera skyddandet av elektroniska data mot piratkopiering i nätverk samt undgå filtreringssystem genom att tillhandahålla sådana data i ett flertal fysiska datorer. Musikverk, filmverk och andra liknande intellektuella skapelser lagras vanligtvis i digital form på elektroniska eller optiska media. Eftersom den digitala lagringsformen medger kopiering och distribution utan kvalitetsförsämring, förekommer omfattande spridning av sådana data över Internet och på andra sätt. Spridningen sker i viss omfattning under kontroll av innehavarna till de rättigheter som är associerade med de intellektuella skapelserna, men i mycket stor omfattning utan sådan kontroll och utan att rättighetsinnehavarna erhåller någon som helst ersättning för det utnyttjande som följer efter spridningen. De intellektuella skapelserna är vanligtvis upphovsrättsligt eller på annat sätt skyddade. Uppfinningen avser även en anordning för att utöva metoden.

TEKNIKENS STÅNDPUNKT

Det har visat sig mycket svårt att helt förhindra oönskad spridning av skyddade verk, trots användning av kopieringsskydd och andra former av elektroniska skydd. Genom användning av Internet och olika former av nätverkssystem, t.ex. av typen peer-to-peer och andra decentraliserade nätverk, har det också visat sig vara möjligt att kringgå vissa lagskydd för upphovsrättsligt skyddade verk, vilka sprids som datafiler.

Ett nätverk av typen peer-to-peer utgör ett decentraliserat nätverk och är uppbyggt så att ett flertal datorer förbinds via ett nät, t.ex. Internet, på sådant sätt att information som finns lagrade i filer i datorerna delas ut och hålls allmänt tillgänglig för användare av nätverket. En för eget bruk avsedd och lagligt kopierad fil, som innehåller en låt eller en videofilm, kan nås från och överföras till en godtycklig dator i nätverket genom så kallad uppladdning av filen.

För att begränsa spridningen av upphovsrättsligt skyddade verk har det föreslagits en metod som bygger på att icke fullständiga datafiler eller datafiler med förvanskat informationsinnehåll sprids medvetet av rättighetsinnehavarna, eller någon annan part. Genom att det efter en sådan spridning förekommer många versioner av ett verk förväntas intresset att anskaffa verk på otillbörligt sätt att minska, eftersom risken att en datafil som laddas hem otillbörligt är skadad är påtaglig.

Ett exempel på hur informationsinnehållet kan förvanskas visas och beskrivs i US2002/0082999. Av patentskriften framgår också generellt hur filer med förvanskat innehåll lagras i flera datorer. Datorerna är anslutna i nätverk av typen peer-to-peer och kan därigenom sprida filerna till andra datorer i nätverket. För att bästa effekt ska uppnås, dvs. att en stor andel av de på nätet tillgängliga filerna är förvanskade, föreslås i US2002/0082999 att spridningen av de förvanskade filerna påbörjas innan datafiler med korrekt innehåll blir tillgängliga. Även om spridningen påbörjas innan någon försäljning av korrekta datafiler, t.ex. i form av CD-skivor och DVD-filmer, satts igång förekommer dock att den korrekta filen börjar spridas ännu tidigare. För att minska effekten av en sådan spridning föreslås i US2002/0082999 att redan från en obehörig källa spridda versioner av en korrekt fil förvanskas på samma sätt och därefter sprids.

De datorer som används för att tillhandahålla, och därigenom sprida, filer med förvanskat innehåll bör förekomma i stort antal, för att spridningen ska vara effektiv. Ett stort antal datorer medför dock större kostnader. Genom att på olika sätt analysera de datorer som sprider filer över t.ex. Internet har det visat sig vara möjligt att lokalisera datorer som används för att sprida förvanskade filer. En analys kan innebära att de tillgängliga filer som finns lagrade i datorn undersöks. Identiteten hos sådana datorer kan definieras av det IP-nummer som datorn använder vid sin kommunikation över Internet. Om IP-numret blir känt, t.ex. genom en fortgående analys av innehåll i utdelade filkataloger, och datorns funktion vid spridningen upptäcks, kan det filtreras bort av andra datorer och därigenom förhindras medverka i spridningen

av förvanskade filer, vilket är en nackdel i arbetet med att försvåra obehörig spridning av datafiler.

UPPFINNINGEN I SAMMANFATTNING

Ett syfte med uppfinningen är att undvika den ovan angivna nackdelen och åstadkomma en metod och en anordning, som möjliggör effektiv spridning av filer med förvanskat innehåll med en begränsad risk för upptäckt. Detta syfte uppnås genom att de datorer som är utförda att sprida filerna tilldelas IP-nummer, vilka väljs ur ett i förhållande till antalet spridande datorer mycket stort antal IP-adresser. Utväljandet sker utan särskild ordning, eller slumpvis, så att inga grupper eller nummerföljder av IP-adresser förekommer. De datorer som sprider de förvanskade filerna fungerar i sammanhanget som stördatorer.

Ett flertal datorer används samtidigt och flera nätverksklienter, dvs. programvaror som delar ut filkataloger och på andra sätt tillhandahåller de förvanskade datafilerna, kan exekveras i stördatorerna. Genom att använda flera nätverksklienter per stördator kan spridningen bringas att öka, utan att flera fysiska datorer behöver användas. Spridningstakten kan bringas att ytterligare öka genom att ett flertal virtuella datorer emuleras i de fysiska datorerna. I ett sådant utförande förses var och en av de virtuella datorerna, eller grupper av virtuella datorer, med IP-adress på det ovan beskrivna sättet. flera datorer kan därvid arbeta med en gemensam IP-adress ut mot nätet.

Ett alternativ eller komplement till emulerade datorer är att genom mjukvara uppfånga identiska nätverksklienters kommunikation med datorernas operativsystem eller funktionsbibliotek och därigenom undvika att olika instanser av programmen hindrar varandras funktion, så att ytterligare fler nätverksklienter kan köras samtidigt per dator.

Lämpligen tunnlas de valda IP-adresserna till stördatorerna för att därigenom ytterligare försvåra spårning av datorerna. Frekvent och oregelbundet byte av IP-adresser förbättrar också möjligheterna att hålla stördatorerna hemliga, så att de inte enkelt kan spåras och spärras. Det kan också vara

lämpligt att använda brandväggar eller annat nätverksskydd mellan stördatorerna och Internet.

KORT BESKRIVNING AV RITNINGARNA

Uppfinningen ska närmare förklaras nedan med hänvisning till bifogade ritningar, vilka

Fig. 1 schematiskt visar ett flertal i ett nät förbundna datorer, i vilka nätverksklienter exekveras för spridning av datafiler, och

Fig. 2 schematiskt visar hur datorer i ett nät kan vara konfigurerade.

UPPFINNINGEN

I en praktisk tillämpning i enlighet med Fig. 1 är ett flertal användardatorer 10 uppkopplade mot Internet 11. Vissa användardatorer fungerar som så kallade supernoder, se beskrivningen nedan med hänvisning till Fig. 2. I användardatorerna exekveras en klientprogramvara, som möjliggör utdelning, uppladdning och nerladdning av datafiler, t.ex. innehållande musik.

De datorer som är anslutna till Internet är alla utifrån sett försedda med en unik IP-adress, vilken normalt tilldelats av den Internetleverantör som användaren utnyttjar. Åtminstone i samband med att en datafil ska överföras mellan två användardatorer är dessa förbundna med varandra, som indikeras i Fig. 1, i sådan omfattning att filöverföring mellan datorerna är möjlig.

Till Internet är också anslutet ett flertal stördatorer 12, vilka kan vara utförda som enskilda fysiska datorer, eller som virtuella datorer. Ett flertal stördatorer är samlade i en så kallad serverpark 19, som är ansluten till Internet via en brandvägg 14. Stördatorerna 12 är också anslutna till Internet och är försedda med IP-adresser. Vid tilldelningen av IP-adresserna undviks sammanhängande sekvenser och på andra sätt sammankopplade IP-adresser. Lämpligen väljs IP-adresser slumpvis ur en stor uppsättning för

vanliga abonnenter avsedda adresser hos en Internetleverantör. IP-adresserna byts också lämpligen ut med oregelbundna intervall för att försvåra spårning och identifiering av stördatorerna. De valda IP-adresserna "tunnlas" in till serverparken.

I det i Fig. 1 visade utförandet exekveras ett flertal klientprogramvaror 13 i stördatorerna 12, vilka kan utgöras av servrar. Klientprogramvarorna 13 kommunicerar med motsvarande klientprogramvara i andra datorer 10 genom Internet och kan därigenom tillhandahålla filer med förvanskat innehåll. Varje klientprogramvara fungerar i detta sammanhang som en störnod.

En klientprogramvara tar normalt endast upp en modern servers fulla kraft under någon procent av den tid programmet är aktivt. Däremellan ligger resursanvändningen på ett fåtal procent. Tyvärr finns dock endast ett fåtal klientprogramvaror av den aktuella typen som kan köras på samma dator samtidigt. För att utnyttja en fysisk dator maximalt och uppnå bästa kostnadseffektivitet bör därför flera virtuella, eller emulerade, datorer köra på varje fysisk dator. Används i ett startskede 35 servrar med 50 virtuella datorer per server uppnås 1750 stördatorer till en bråkdel av vad det annars hade kostat i inköp, drift, mm.

En av stördatorerna utgörs av en fysisk dator och i denna exekverande emuleringsprogramvara. Emuleringsprogramvaran får den fysiska enda stördatorn att uppträda som ett flertal virtuella datorer 15. De virtuella datorerna kan i sin tur vardera exekvera ett flertal klientprogramvaror och därigenom ytterligare öka antalet verksamma störnoder.

Förekommande protokoll för spårning av datorer, t.ex. ICMP TRACEROUTE, förhindras genom användning av brandvägg och/eller störprogramvara att detektera stördatorn.

En första godtycklig dator 16, som exekverar en klientprogramvara för kommunikation mellan datorer anslutna i nät av typen peer-to-peer, kan vara ansluten till en stördator med en första störnod 17. Det bör noteras att med nät av typen peer-to-peer avses i detta sammanhang också funktionsmässigt snarlika fildelningsnät. Genom det för störnoden valda IP-numret synes datorn 16 vara förbunden med en annan fiktiv dator 18, men är alltså via

brandväggen 14 förbunden med en dator i serverparken 19. På motsvarande sätt är en andra godtycklig dator 20 förbunden med en andra störnod 21, men synes vara förbunden med en fiktiv dator 22, och en tredje godtycklig dator 23 med en tredje störnod 24, även om den kan uppfattas vara förbunden med ytterligare en fiktiv dator 25.

I samband med att en förvanskad fil överförs från en störnod registreras överföringen. Lagring av data som avser överföringar sker i en databas 26 i serverparken. Störnoderna styrs via en centralenhet 27 i serverparken. Centralenheten 27 läser av data som lagrats i databasen 26 och beräknar spridningseffekt och andra relevanta utfall av störnodernas arbete. Beräknad och upptagen information lagras också lämpligen efterhand i databasen.

Fig. 2 visar schematiskt hur ett decentraliserat nät kan se ut. Ett flertal datorer 10 ingår i nätet och är organiserade i nodgrupper 29 runt så kallade supernoder 28. En dator 10 når andra datorer för överföring av datafiler på ovan beskrivet sätt endast genom den supernod 28 datorn är ansluten till. Vanligen är en dator ansluten till endast en supernod. Den första störnoden 17 är förbunden med en supernod 28 på samma sätt som övriga med supernoden förbundna datorer och uppträder på samma sätt som en sådan dator, både mot andra datorer och mot supernoden. På motsvarande sätt är den andra störnoden 21 och den tredje störnoden 24 förbundna med supernoder 28. Det kan förekomma att flera störnoder 24 associeras, eller förbinds, med samma supernod, eftersom konfigurationen sker helt utan kännedom om och utan hänsyn till vilka datorer som är störnoder.

Störnoderna styrs via centralenheten 27 och information som finns lagrad i databasen 26. Inprogrammerade block av aktiviteter kan aktiveras antingen för enskilda noder, för grupper av noder, eller för samtliga noder. Exempel på sådana aktiviteter kan vara att byta supernod, eller att starta om den virtuella datorn. Den mjukvara som används i störnoderna och de virtuella datorerna är lämpligen identisk för att enkelt kunna uppdateras med hjälp av konventionella eller särskilt anpassade nätverksverktyg.

För att mäta effektiviteten hos störningarna kan det via slumpmässiga, eller valda, supernoder sökas efter de verk som skyddas. Sedan jämförs

data i sökresultaten med och en procentuell effektivitet kan räknas fram. Här kan även ses hur stor den sekundära störeffekten, så kallad "piggybacking", är, det vill säga den effekt som uppkommer då många som laddar ned filer med förvanskat innehåll i jakten efter "riktiga" filer inte orkar ta bort filerna och därmed själva fungerar som externa störnoder. Den sekundära störeffekten kan därefter läggas till tidigare framtaget värde och resultat, som t.ex. totalt antal nedladdade filer med förvanskat innehåll, kan räknas fram och presenteras som statistik.

PATENTKRAV

1. Metod för att effektivisera skyddandet av elektroniska data mot piratkopiering i nätverk samt undgå filtreringssystem genom att tillhandahålla sådana data i ett flertal fysiska datorer (12), *kännetecknad* av

att en andra uppsättning filer med i förhållande till en första uppsättning filer förvanskat informationsinnehåll tillgängliggörs för datorerna (12),

att datorerna tilldelas IP-adresser utan inbördes ordningsföljd valda ur en uppsättning IP-adresser, varvid uppsättningen IP-adresser är mångfalt större än antalet valda IP-adresser,

att ett flertal nätverksklienter (13) exekveras i datorerna, varvid en nätverksklient är utförd att ansluta till ett nätverk av typen peer-to-peer, eller motsvarande nätverk, och

att den andra uppsättningen filer görs tillgänglig för nedladdning till andra till nätverket anslutna datorer.

2. Metod i enlighet med krav 1, varvid flera nätverksklienter exekveras i ett flertal fysiska datorer genom emulering av flera virtuella datorer.

3. Metod i enlighet med krav 1, varvid flera nätverksklienter exekveras i ett flertal fysiska datorer genom uppfångande av nätverksklientens kommunikation med ett i de fysiska datorerna exekverande operativsystem och tillhörande funktionsbibliotek.

4. Metod i enlighet med krav 1, varvid ett flertal identiska nätverksklienter exekveras i samma fysiska eller virtuella dator genom uppfångande av nätverksklientens funktionsanrop till ett i den fysiska datorern exekverande operativsystem och tillhörande funktionsbibliotek.

5. Metod i enlighet med krav 1, varvid datorerna fortlöpande förses med nya utan sekvenser eller närliggande grupperingar uppvisande IP-adresser.

6. Metod i enlighet med krav 1, varvid relevanta svarsdata i tillämpliga nätverksprotokoll spärras och/eller modifieras vid kommunikation mellan nätverksklienterna (13) och andra till nätverket anslutna datorer för att dölja faktisk fysisk placering.

7. Metod i enlighet med krav 1, varvid flera datorer delar på en IP-adress.

8. Metod i enlighet med krav 1, varvid ett flertal virtuella datorer (15) emuleras i fysiska datorer, de virtuella datorerna (15) tilldelas IP-adresser utan inbördes ordningsföljd valda ur en uppsättning IP-adresser, och varvid uppsättningen IP-adresser är mångfalt större än antalet valda IP-adresser.

9. Metod i enlighet med krav 8, varvid data beträffande nedladdning av filer med förvanskat informationsinnehåll från nätverksklienter lagras i en central databas (26).

10. Anordning för spridning av elektroniskt lagrade data, innefattande ett flertal sådana data tillhandahållande fysiska datorer (12),
kännetecknad av
att de fysiska datorerna är tilldelade IP-adresser utan inbördes ordningsföljd valda ur en uppsättning IP-adresser, varvid uppsättningen IP-adresser är mångfalt större än antalet valda IP-adresser,
att de fysiska datorerna är ordnade i en serverpark (19) och
att serverparken innefattar en centralenhet (27) och en av centralenheten (27) styrd databas (26).

SAMMANDRAG

Metod för spridning av elektroniskt lagrade data genom att tillhandahålla sådana data i ett flertal fysiska datorer (12). En andra uppsättning filer med i förhållande till en första uppsättning filer förvanskat informationsinnehåll lagras i de fysiska datorerna (12). De fysiska datorerna tilldelas IP-adresser utan inbördes ordningsföljd valda ur en uppsättning IP-adresser, varvid uppsättningen IP-adresser är mångfalt större än antalet valda IP-adresser. Ett flertal nätverksklienter (13) exekveras i de fysiska datorerna, varvid en nätverksklient är utförd att ansluta till ett nätverk av typen peer-to-peer, och den andra uppsättningen filer görs tillgänglig för nedladdning till andra till nätverket anslutna datorer.

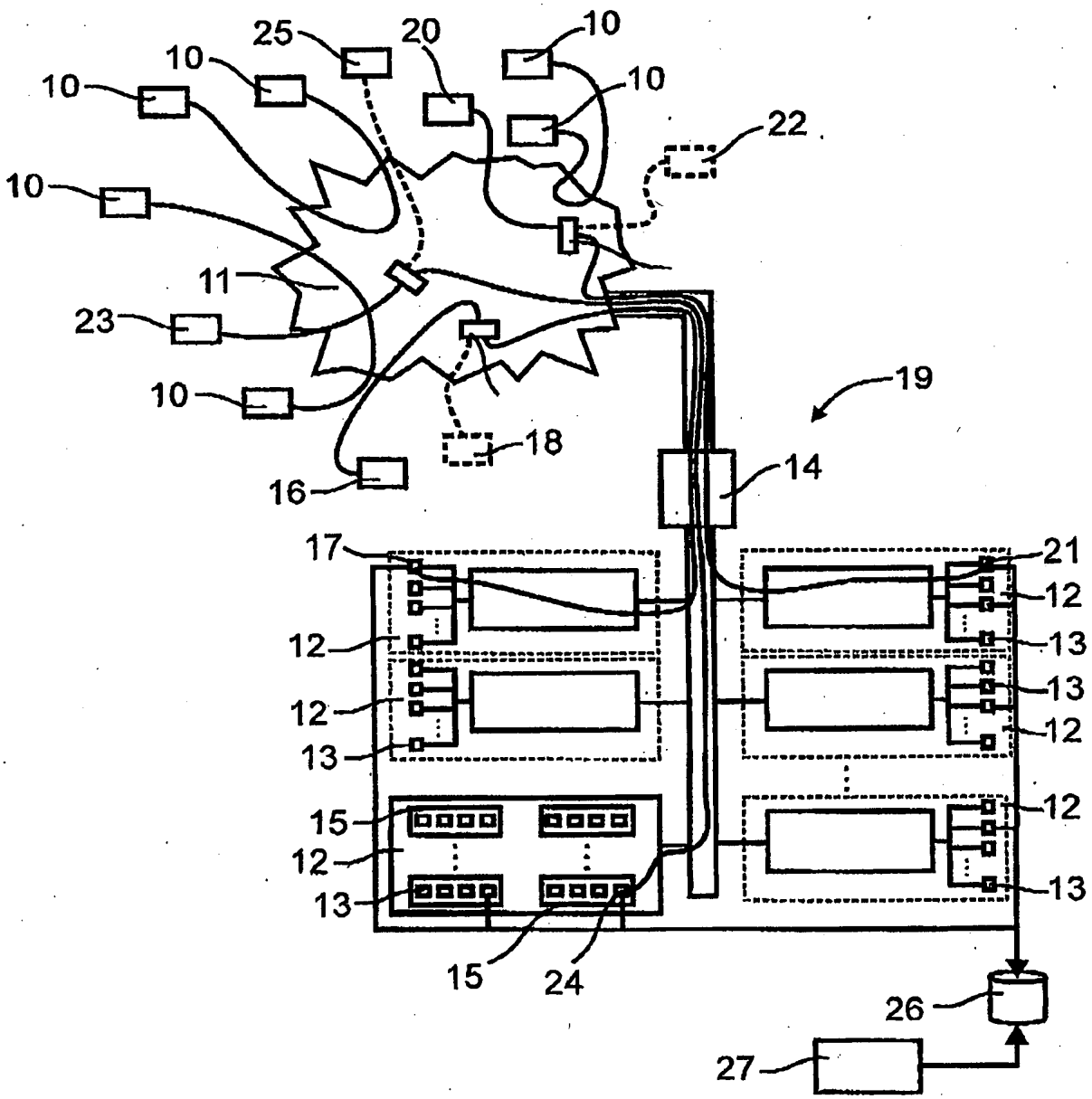

Fig. 1

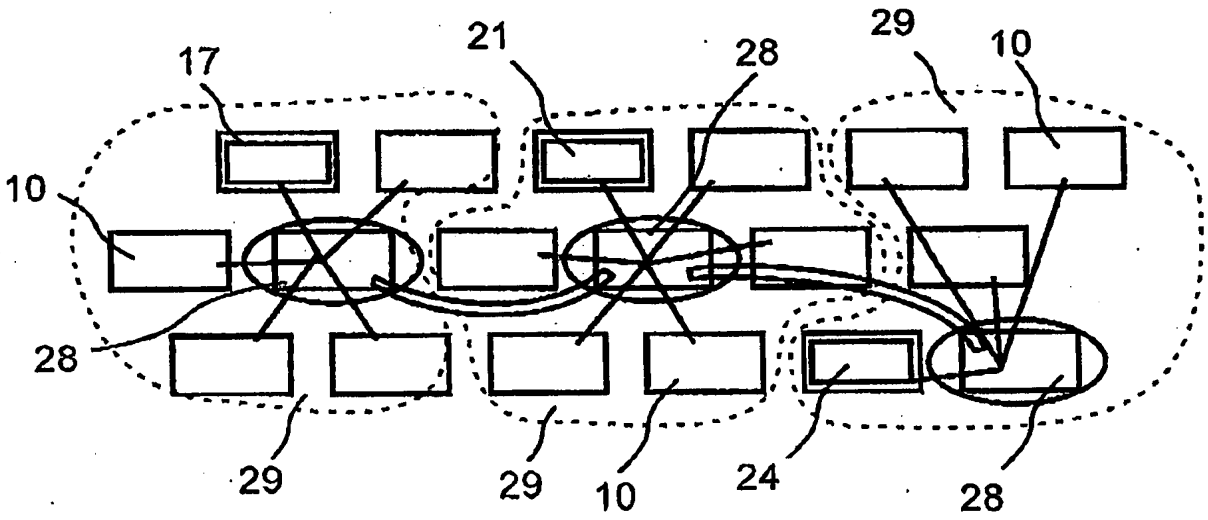

Fig. 2